

Mr. Chairman, Senator Hollings, and other Members of the Subcommittee, I want to thank you for this opportunity to testify on the recent Internet Denial of service attacks and the federal response to these incidents, with a particular focus on the challenges facing the Department of Justice in its fight against cybercrime. At a time where new technologies abound and our society becomes increasingly reliant on computer networks and thus vulnerable to cybercrime, we look forward to working with Congress to ensure that law enforcement, in cooperation with the private sector, can play an appropriate and critical role in protecting the well-being of Americans while also respecting fundamental notions of individual privacy that we hold dear in this country.

### **Comments on the Recent Attacks**

I would be happy to address your questions on the recent attacks, to the extent I can do so without compromising our investigation. At this point, I would simply say that we are taking the attacks very seriously and that we will do everything in our power to identify those responsible and bring them to justice. In addition to the malicious disruption of legitimate commerce, so-called Denial of service attacks involve the unlawful intrusion into an unknown number of computers, which are in turn used to launch attacks on the eventual target computer, in this case the computers of Yahoo, eBay, and others. Thus, the number of victims in these types of cases can be substantial, and the collective loss and cost to respond to these attacks can run into the tens of millions of dollars or more.

### **Overview of Investigative Efforts and Coordination**

Computer crime investigators in a number of FBI field offices and investigators from other agencies are investigating these attacks. They are coordinating information with the National Infrastructure Protection Center (NIPC) of the FBI. The agents are also working closely with our network of specially trained computer crime prosecutors who are available 24 hours a day/7 days a week to provide legal advice and obtain whatever court orders are necessary. Attorneys from the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) are coordinating with the Assistant United States Attorneys in the field. We are also obtaining information from victim companies and security experts, who, like many in the Internet community, condemn these recent

attacks. We are also working closely with our counterparts in other nations. I am proud of the efforts being made in this case, including the assistance we are receiving from a number of federal agencies.

### **The Emergence of Cybercrime**

It is worth remembering that just ten years ago, the Internet was largely unknown and unavailable to the average person. There was no e-commerce, no e-Bay, no amazon-dot-com. At that time, the Internet was a collection of military, academic, and research networks serving a small community of trusted users. That world is history. The far-reaching, ever-expanding, and ever more rapid advances in computer and software technology over the last ten years have combined with the explosive growth of the Internet to change the world forever. For the most part, the Internet and other technologies are providing wonderful benefits to our society B from providing new, high-wage jobs to our economy, to expanding educational opportunities, improving health care, and allowing family and friends to keep in touch in ways that were simply impossible a decade ago.

Unfortunately, these wonderful technologies also provide new opportunities for criminals. Online crime is rapidly increasing. We are seeing more "pure" computer crimes, that is, crimes where the computer is used as a weapon to attack other computers, as we saw in the distributed denial of service attacks I just spoke about, and in the spread of malicious code, like viruses. Our vulnerability to this type of crime is astonishingly high B it was only this past December that a defendant admitted, when he pled guilty in federal and state court to creating and releasing the Melissa virus, that he caused over 80 million dollars in damage. These crimes also include computer intrusions designed to obtain information of the most sensitive sort B such as credit cards, companies=trade secrets, or individuals= private information.

These crimes not only affect our financial well-being and our privacy; they also threaten our nations critical infrastructure. Our banking system, the stock market, the electricity and water supply, telecommunications networks, and critical government services, such as emergency and national defense services, all rely on computer networks. For a real-world terrorist to blow up a dam, he would need tons of explosives, a delivery system, and a surreptitious means of evading armed security guards. For a cyberterrorist, the same devastating result could be achieved by hacking into the control network and

commanding the computer to open the floodgates.

We are also seeing a migration of "traditional" crimes **B** including threats, child pornography, fraud, gambling, and extortion **B** from the physical to the online world. When these crimes are carried out online, perpetrators often find that they can reach more victims quickly and quite easily, turning what were once "local" scams into crimes that cross interstate and international borders. Computers and computer networks provide a cheap and powerful means of communications, and criminals take advantage of this just like everyone else. In addition, sophisticated criminals can readily use the easy anonymity that the Internet provides to hide their crimes.

### **Challenges of Cybercrime**

The Internet and computers have brought tremendous benefits to our society, including greater freedom of expression and economic growth. But we must also recognize that as a result of our society's increasing reliance on technology, investigators and prosecutors at all levels **B** international, federal, state, and local **B** are encountering unique challenges. These challenges generally can be divided into three categories:

- 1) Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;
- 2) Legal challenges resulting from laws and legal tools needed to investigate cybercrime lagging behind technological, structural, and social changes; and
- 3) Resource challenges to ensure we have satisfied critical investigative and prosecutorial needs at all levels of government.

Before I discuss each of these challenges, let me say that we recognize that we in government will not be able to solve all of these problems. In fact, we believe strongly that the private sector should take the lead in protecting private computer networks, through more vigilant security efforts, information sharing, and, where appropriate, cooperation with government agencies. The private sector has the resources, the technical ability, and the trained personnel to ensure that, as technology continues to develop and change rapidly, the Internet is a safer place for all of us. The private sector can and should take the lead on improving security practices and the development of a more secure Internet

infrastructure.

However, even assuming that private sector, and the broader Internet community as a whole, take steps to provide a safe, secure, and vibrant Internet, there will be instances where the practices and safeguards fail. Criminals rob banks even though banks use numerous security measures. In such cases, law enforcement must be prepared and equipped to investigate and prosecute cybercriminals in order to stop their criminal activity, to punish them, and to deter others who might follow the same path. This is the reason that it is so important that we work together to address the challenges I am about to discuss.

### ***Technical Challenges***

When a hacker disrupts air traffic control at a local airport, when a child pornographer sends computer files, when a cyberstalker sends a threatening e-mail to a public school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. Everything on the Internet is communications, from an e-mail to an electronic heist. Finding an electronic criminal means that law enforcement must determine who is responsible for sending an electronic threat or initiating an electronic robbery. To accomplish this, law enforcement must in nearly every case trace the "electronic trail" leading from the victim back to the perpetrator.

Tracking a criminal online is not necessarily an impossible task, as demonstrated last year when federal and state law enforcement agencies were able to track down the creator of the Melissa virus and the individual who created a false Bloomberg News Service website in order to drive up the stock price of PairGain, a telecommunications company in California. In both cases, technology enabled us to find the individuals who were engaging in criminal activity.

Unfortunately, despite our successes in the Melissa and PairGain cases, we still face significant challenges as online criminals become more sophisticated, often wearing the equivalent of Internet electronic gloves to hide their fingerprints and their identity.

It doesn't take a master hacker to disappear on a network. Ironically, while the public is justifiably worried about protecting the legitimate electronic privacy of individuals who use networks, a

criminal using tools and other information easily available over the Internet can operate in almost perfect anonymity. By weaving his or her communications through a series of anonymous remailers; by creating a few forged e-mail headers with powerful, point-and-click tools readily downloadable from many hacker web sites; or by using a free-trial account or two, a hacker, online pornographer, or web-based fraud artist can often effectively hide the trail of his or her communications.

As we consider the challenge created by anonymity, we must also recognize that there are legitimate reasons to allow anonymity in communications networks. A whistleblower, a resistance fighter in Kosovo, a battered woman's support group - all of these individuals may understandably wish to use the Internet and other new technologies to communicate with others without revealing their identities.

In addition to problems related to the anonymous nature of the Internet, we are being challenged to investigate and prosecute criminals in an international arena. The Internet is a global medium that does not recognize physical and jurisdictional boundaries. A criminal no longer needs to be at the actual scene of the crime to prey on his or her victims. As a result, a computer server running a web page designed to defraud U.S. senior citizens might be located in Europe or Asia. A child pornographer may distribute photographs or videos via e-mail, sending the e-mails through the communications networks of several countries before they reach their intended recipients. With more than 190 Internet-connected countries in the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail might, in certain circumstances, end as soon as he or she disconnects from the Internet.

Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network. In certain circumstances, the fact that the evidence is stored and held by a third party, such as an internet service provider, might be helpful to law enforcement agencies who might be able to use lawful process to get that information. However, storing information remotely can also create a challenge to law enforcement, which cannot ignore the real-world limits of local, state, and national sovereignty and jurisdiction. Obtaining information from foreign countries, especially on an expedited basis, can be a

daunting task, especially when a country may be in a different time zone, use a different language, have different legal rules, and may not have trained experts available. Consequently, even as the Internet and other new technologies have given us new abilities to find criminals remotely, our abilities can be hindered if we cannot obtain the necessary legal cooperation from our counterparts in other countries.

The vast majority of Internet companies are good corporate citizens and are interested in the safety of our citizens. In fact, several companies have been engaged in discussions with law enforcement regarding our concerns. Despite these efforts, we have learned that we cannot take for granted the nature of any Internet service providers' services, its record-keeping practices, and its ability or willingness to cooperate with us. We have encountered a handful of companies involved in criminal activity. In addition, even those companies that are not involved in criminal activities might not be able to assist us because of business reasons or privacy concerns that have resulted in them not keeping the records that will assist in the investigation of a particular crime.

Moreover, users connect to the Internet from anywhere in the world over old-fashioned telephone lines, wireless phones, cable modems, and satellite systems. Each of these telecommunications systems has its own protocols for addressing and routing traffic, which means that tracking all the way back to the criminal at his or her computer will require agents to be fluent in each technical language. Gathering this evidence from so many kinds of providers is a very different proposition from the days when we simply obtained an order for a telephone company to trace a threatening call.

### ***Legal Challenges***

Deterring and punishing computer criminals requires a legal structure that will support detection and successful prosecution of offenders. Yet the laws defining computer offenses, and the legal tools needed to investigate criminals using the Internet, can lag behind technological and social changes, creating legal challenges to law enforcement agencies.

We may be able to correct some of the legal challenges we encounter through legislative action. For example, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, arguably does not reach a computer hacker who causes a large amount of damage to a network of computers if no individual

computer sustains over \$5,000 worth of damage. The Department of Justice has encountered several instances in which intruders have gained unauthorized access to protected computers (whether publicly or privately owned) used in the provision of critical infrastructure systems and services such as those that hospitals use to store sensitive information and to treat patients, and those that the military uses to defend the nation but where proof of damage in excess of \$5000 has not been readily available.

The laws under which we are able to identify the origin and destination of telephone calls and computer messages also need to be reviewed. For example, under current law we may have to obtain court orders in multiple jurisdictions to trace a single communication. Obtaining court orders in multiple jurisdictions does not advance any reasonable privacy safeguard, yet it can be a substantial impediment to a fast-paced investigation. As the Attorney General testified recently, it might be extremely helpful, for instance, to provide nationwide effect for trap and trace orders.

Another concern focuses on the problem of online threats and serious harassment -- that is, cyberstalking. Current federal law does not address those situations where a cyberstalker uses unwitting third parties to bombard a victim with messages, transmits personal data about a person such as the route by which the victim's children walk to school in order to place such person or his family in fear of injury, or sends an e-mail or other communications under someone else's name with the intent to abuse, harass, or threaten that person. We believe federal law may need to be amended to address this gap.

These aren't hypothetical changes that we are proposing to address. Just ask the California woman who was awakened six times in the middle of the night to find men knocking on her door offering to rape her. She discovered that a man whom she had told she was not romantically interested in had posted personal advertisements on a variety of Internet services pretending to be her. Each posting, which contained her home address and telephone number, claimed that she fantasized about being raped. We need to ensure that laws against harassment clearly prohibit such horrific actions, particularly since access to the Internet means immediate access to a wide audience.

While we believe changes in federal law may be necessary to address these challenges, we also

want to emphasize that any such legislation should be tailored to address the challenges we face and should avoid unnecessary infringement on personal privacy. We recognize the importance the public attaches to individual privacy, and any legislation must be carefully balanced to avoid unnecessary infringement on the privacy rights we hold dear in this country.

### ***Resource Challenges***

In addition to technical and legal challenges, we face significant resource challenges. Simply stated, we need an adequate number of prosecutors and agents **B** at the federal, state and local level **B** trained with the necessary skills and properly equipped to effectively fight all types of cybercrime.

While Congress has been very supportive of the Department's cybercrime efforts, we need additional resources to ensure we are adequately equipped to continue our battle against cybercriminals. The President has requested \$37 million in new money in FY 2001 to expand our staffing, training and technological capabilities to continue the fight against computer crime. Together, these enhancements will increase the Department's 2001 funding base for computer crime to \$138 million, 28 percent more than in 2000.

Last, the Department of Justice would like to work with Congress to develop a comprehensive, five-year plan **B** with FY 2001 as our baseline **B** to prevent cybercrime and, when it does occur, to locate, identify, apprehend and bring to justice those responsible for these types of crimes. On February 16th, the Attorney General testified before Congress regarding a proposed a 10-point plan to identify the key areas we need to develop for our cybercrime capability. The key points of this plan she touched upon include:

- C      Developing a round-the-clock network of federal, state and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime.
- C      Developing and sharing expertise **B** personnel and equipment **B** among federal, state and local law enforcement agencies.
- C      Dramatically increasing our computer forensic capabilities, which are so essential in computer crime investigations **B** both hacking cases and cases where computers are

used to facilitate other crimes, including drug trafficking, terrorism, and child pornography.

C Reviewing whether we have adequate legal tools to locate, identify, and prosecute cybercriminals. In particular, we may need new and more robust procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions.

We also need to explore whether we have adequate tools at the federal level to effectively investigate cybercrime.

C Because of the borderless nature of the Internet, we need to develop effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations. A balanced international strategy for combating cybercrime should be at the top of our national security agenda.

C We need to work in partnership with industry to address cybercrime and security. This should not be a top-down approach through excessive government regulation or mandates. Rather, we need a true partnership, where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy.

C And we need to teach our young people about the responsible use of the Internet. The Department of Justice and the Information Technology Association of America have already taken steps to do so through the development of the Cybercitizen Partnership, but more needs to be done.

## **Efforts Against Cybercrime**

Despite the technical, legal, and resource challenges, the Department has made strides in our fight against cybercrime. We have and will continue to develop extensive investigatory and prosecutorial programs to counter cybercrime. Let me take a few moments to details some of our efforts to date.

On the investigatory side, we have the FBI's National Infrastructure Protection Center (NIPC) and specialized squads located in 16 field offices.

On the prosecutorial side, we have trained attorneys, both in headquarters and in the field, who

are experts in the legal, technological, and practical challenges involved in investigating and prosecuting cybercrime. The cornerstone of our prosecutor cybercrime program is the Computer Crime and Intellectual Property Section. CCIPS, which currently has 18 attorneys, was founded in 1991 as the Computer Crime Unit and was elevated to Section status in 1996. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as AComputer and Telecommunications Coordinators@ (CTC=s) in U.S. Attorneys= Offices around the country. Each CTC is given special training and equipment, and serves as the district=s expert in computer crime cases. As a result of these programs, the number of cases and prosecutions by the Department is growing at a tremendous rate. For example, in 1998, US Attorneys= Offices filed 85 computer crime cases against 116 defendants. This represents a 29% increase in the number of cases filed and a 51% increase in the number of defendants, compared to the previous year. During that same period of time, a total of 62 cases against 72 defendants were terminated, with 78% of those defendants being convicted.

At the same time, our prosecutors are working with numerous other federal, state, and local investigators and prosecutors, providing assistance in any case involving computers and other high technology, such as computer searches and seizure. In sum, the Department and, in particular, its investigators and prosecutors take seriously our responsibility to protect the nation=s computers and the Internet from computer crime.

In addition to the Department=s efforts, other agencies including the Customs Service, the Secret Service, the Securities and Exchange Commission, and the U.S. Postal Service=s Inspectors General, have played a role in the investigation and prosecution of computer crimes.

### **Infrastructure Protection**

The Department is also a full partner in ongoing efforts to assure our nation=s critical infrastructures and to make them less vulnerable to the emerging risks of the information age.

I mentioned before that we believe strongly that the private sector should take the lead in protecting private computer networks, through more vigilant security efforts, information sharing, and, where appropriate, cooperation with government agencies. Within this framework, and apart from prosecuting those who launch criminal attacks on our infrastructure (which is our critical responsibility),

the Department can make important contributions. In the information sharing arena, we have continued some of the groundwork started by the President's Commission on Critical Infrastructure Protection by more closely examining the issues that may impede robust sharing of risk-related information between private sector entities, between governmental entities, and between government and the private sector.

As the private sector protects its networks, so must the government. Therefore, the Department of Justice is working to ensure that its own networks are secure. We are also involved in efforts, under the auspices of the Critical Infrastructure Coordinating Group of the National Security Council, to help federal agencies expedite and simplify the process of performing vulnerability assessments, in order to uncover hidden vulnerabilities of critical government systems before others try to do that for us.

Finally, the Justice Department also is involved in efforts to ensure that all programs arising out of the federal government's infrastructure assurance efforts are implemented in way entirely respects long-standing protections for the privacy rights of individuals.

## **Conclusion**

On behalf of the Department of Justice, I want to thank Congress for all the support it has given to our efforts to combat cybercrimes. Advancements in technology indicate that our efforts are only just beginning. We look forward to working with Congress and the private sector to ensure that we have a robust and effective long-term plan for combating cybercrime, protecting our nation's infrastructure, safeguarding privacy, and ensuring that the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society.